UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/509,876	04/04/2005	Marc Joye	032326-285	4960

21839 7590 09/24/2008

BUCHANAN, INGERSOLL & ROONEY PC
POST OFFICE BOX 1404
ALEXANDRIA, VA 22313-1404

EXAMINER	
REVAK, CHRISTOPHER A	

ART UNIT	PAPER NUMBER
2131	

NOTIFICATION DATE	DELIVERY MODE
09/24/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ADIPFDD@bipc.com

Office Action Summary	Application No.	Applicant(s)	
	10/509,876	JOYE ET AL.	
	Examiner	Art Unit	
	Christopher A. Revak	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *04 October 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *2-24* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *2-9,19-24* is/are rejected.

7)☒ Claim(s) *10-18* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *04 October 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Priority

1. Acknowledgment is made of applicant's claim for foreign priority under 35 U.S.C. 119(a)-(d).

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claims 2-9 and 19-24 are rejected under 35 U.S.C. 102(e) as being anticipated by Vadekar et al, U.S. Patent 7,020,281.

As per claim 2, it is taught wherein the predefined number is variable from one predefined block of instructions to another (col. 4, line 31 through col. 5, line 4).

As per claim 3, it is disclosed wherein the common set of instructions comprises at least one calculation instruction that is equivalent to a calculation instruction of each predefined block in the context of a covert channel attack (col. 4, lines 3-14).

As per claim 4, it is taught wherein the common set of instructions also comprises an instruction to update a loop pointer indicating a number of executions

already performed with the common set of instructions (col. 4, line 31 through col. 5, line 4).

As per claim 5, it is disclosed wherein the common set of instructions also comprises an instruction to update a state pointer indicating whether the predefined number has been reached (col. 4, line 31 through col. 5, line 4).

As per claim 6, it is taught wherein the value of the loop pointer is a function of the value of the input variable and/or number of instructions in the selected block of instructions (col. 4, line 31 through col. 5, line 4).

As per claim 7, it is disclosed wherein in order to successively effect several blocks of instructions chosen from amongst the plural predefined block of instructions, each selected block of instructions is selected as a function of an input variable associated with an input index (col. 4, line 31 through col. 5, line 4).

As per claim 8, it is taught wherein one and the same block of instructions is selected several times according to the input variable associated with the input index (col. 4, line 31 through col. 5, line 4).

As per claim 9, it is disclosed wherein at least two of the following data items, (a) the value of a loop pointer, (b) the value of a state pointer, (c) the value of the input variable, and (d) the number of instructions of the selected block of instructions are linked by one or more mathematical functions (col. 4, line 31 through col. 5, line 4).

As per claim 19, it is taught of a method for obtaining an elementary set of instructions common to a plurality of predefined blocks of instructions, for implementing a cryptographic calculation method according to claim 21, comprising the following

steps E1: breaking down each predefined block of instructions into a series of elementary blocks that are equivalent in the context of a covert channel attack, and classifying all the elementary blocks, E2: identifying a common elementary block that is equivalent to all the elementary blocks of all the predefined blocks of instructions, E3: identifying a common block comprising at least the common elementary block previously identified and an instruction to update a loop pointer such that an execution of the common elementary block associated with the value of the loop pointer and an execution of the elementary block with a rank equal to the value of the loop pointer are identical (col. 3, lines 26 through col. 4, line 2; col. 4, lines 3-14; and col. 4, line 31 through col. 5, line 4).

As per claim 20, it is disclosed wherein, during step E1, at least one fictional instruction is added to at least one predefined block of instructions (col. 4, line 31 through col. 5, line 4).

As per claim 21, it is taught of a method for implementing a cryptographic calculation in an electronic device, comprising the following steps selecting a block of instructions from amongst a plurality of predefined blocks of instructions, as a function of an input variable; and executing a set of instructions that is common to the plurality of predefined blocks of instructions a predefined number of times, wherein said predefined number is associated with the selected block of instructions (col. 3, lines 26 through col. 4, line 2 and col. 4, line 31 through col. 5, line 4).

As per claim 22, it is disclosed of wherein the value of the state pointer is a function of the value of the input variable and/or of the number of instructions in the selected block of instructions (col. 4, line 31 through col. 5, line 4).

As per claim 23, it is taught wherein said several inputs comprise a matrix (col. 4, line 31 through col. 5, line 4).

As per claim 24, it is disclosed wherein said electronic device is a chip card (col. 4, line 25).

Allowable Subject Matter

4. Claims 10-18 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christopher A. Revak whose telephone number is 571-272-3794. The examiner can normally be reached on Monday-Friday, 9:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Christopher A. Revak/
Primary Examiner, Art Unit 2131